

RECEIVED
CENTRAL FAX CENTER

Appl. No. 09/536,945
Appeal Brief Cover Letter

OCT 18 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Epstein et al.

Serial No.: 09/536,945

Filed: 3/28/2000

Title: **PROTECTING CONTENT MATERIAL FROM ELICIT REPRODUCTION
BY PROOF OF EXISTANCE OF A COMPLETE DATA SET USING SECURITY
IDENTIFIERS**

Atty. Docket No.: US-000032

Group Art Unit: 2134

Examiner: Tran, Tongoc

Mail Stop: **APPEAL BRIEF - PATENTS**

Commissioner for Patents

Alexandria, VA 22313-1450

Sir:

Enclosed is an Appeal Brief in the above-identified application.

☒ A credit card authorization in the amount of \$340 is enclosed.

☐ The Commissioner has already been authorized to charge fees in this application to Deposit Account .

☐ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account _____. Enclosed is a copy of this sheet.

Respectfully submitted,



Robert M. McDermott, Esq.

Reg. No. 41,508

804-493-0707

CERTIFICATE OF MAILING OR FACSIMILE TRANSMISSION

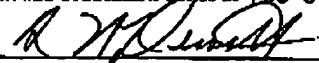
It is hereby certified that this correspondence is

|| being deposited with the United States Postal Service as first-class mail in an envelope addressed to:
Mail Stop Appeal Brief- Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450;

☒ transmitted by facsimile to the U.S. Patent and Trademark Office at 703-872-9306.

On 18 October 2004

By



Atty. Docket No. US-000032

RECEIVED
CENTRAL FAX CENTER

OCT 18 2004

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of Epstein et al.

Atty. Docket No.: US-000032

Serial No.: 09/536,945

Group Art Unit: 2134

Filed: 3/28/2000

Examiner: Tran, Tongoc

**Title: PROTECTING CONTENT MATERIAL FROM ELICIT REPRODUCTION
BY PROOF OF EXISTANCE OF A COMPLETE DATA SET USING SECURITY
IDENTIFIERS**

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37

Commissioner for Patents

Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of the Examiner dated 7 June 2004, finally rejecting claims 1-40 of the subject application.

I. REAL PARTY IN INTEREST

The above-identified application is assigned, in its entirety, to Philips Electronics North America Corporation, a company organized under the laws of the State of Delaware.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.

10/19/2004 MAHMED1 00000016 09536945

01 FC:1402

340.00 OP

III. STATUS OF CLAIMS

Claims 1-40 are pending in the application.

Claims 1-40 stand rejected by the Examiner under 35 U.S.C. 103(a).

These rejected claims are the subject of this appeal.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection in the Office Action dated 7 June 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention is designed to prevent the rendering of portions of a data set, if the entire data set is not present. In an exemplary embodiment, the invention prevents the playback of songs that are "ripped" from an album that is protected by the techniques of this invention. An entirety parameter that is based on a plurality of security identifiers associated with data items in the data set is communicated with the data set, and this entirety parameter is used to verify that the data items associated with the entirety parameter are present when a data item is selected for rendering. (Applicants' page 5, lines 12-27.) Preferably, the entirety parameter is a hash value of a composite of the security identifiers (page 7, lines 20-21), so that if any of the security identifiers forming the entirety parameter is absent or modified in a subsequent copy, a determined entirety value from this copy will not match the original entirety parameter (page 12, lines 15-24). In a preferred embodiment, multiple entirety parameters are communicated with the data set, each entirety parameter being associated with a different subset of data items in the data set (page 10, line 16 through page 11, line 6). Before or during the rendering of a data item, an entirety value is determined based on the security identifiers associated with the select entirety parameter, and if the determined entirety value does not correspond to the select entirety parameter, thereby indicating that the data items associated with the security identifiers are not present or have been modified, the rendering is terminated (Applicants' page 9, lines 18-27).

As claimed in independent claim 1, the invention comprises a method for discouraging theft of content material (Applicants' FIG. 3; page 11, line 7 through page 12, line 3). A plurality of data items comprising the content material is collected to form a data set (loop 310-335 of FIG. 3; page 11, lines 8-18). Each of the data items have an associated security identifier that is configured such that a modification of the data item effects a modification of the security identifier, and an entirety parameter is created that is based on a plurality of the security identifiers (352 of FIG. 3; page 11, line 28 through page 12, line 1). The entirety parameter is included in the data set, so that if an entirety of the data set is determined not to be present, the processing of data items in the data set can be terminated (354 of FIG. 3; page 12, lines 2-3).

As claimed in dependent claim 8, the invention comprises creating a plurality of other entirety parameters, each of the plurality of other entirety parameters being based on an associated plurality of security identifiers, and including the plurality of other entirety parameters in the data set (loop 350-359 of FIG. 3; page 11, line 20 through page 12, line 3). Preferably, each entirety parameter corresponds to a subset of the security identifiers, so that a determination of whether the entirety of the data set is likely to be present can be performed quickly (page 10, lines 19-24). The confidence level associated with the likelihood that the entirety of the data set is present can be increased by testing for the presence of data items corresponding to multiple entirety parameters, as time permits (loop 410-455 of FIG. 4; page 12, lines 21-28).

As claimed in independent claim 9, the invention comprises a method of decoding content material from a source (FIG. 4; page 12, lines 4-30), that includes reading the entirety parameter (420 of FIG. 4) and the security identifiers (430 of FIG. 4) from the source, determining an entirety value based on the security identifiers (440 of FIG. 4), and rendering (460) the content material based on a correspondence (445 of FIG. 4) between the determined entirety value and the entirety parameter read from the source.

As claimed in dependent claim 10, the entirety parameter is randomly selected from a set of entirety parameters (410 of FIG. 4), each entirety parameter of the set of entirety parameters having an associated set of security identifiers ($W(e,1) \dots W(e,m)$). As noted above, each of the entirety parameters corresponds to a subset of the security

identifiers in the data set, thereby allowing for a faster determination of whether the data items corresponding to the entirety parameter are present at the source (page 10, lines 16-24).

As claimed in independent claim 17, the invention comprises a storage medium (130 of FIG. 1) that is configured to contain content material. The storage medium comprises a data structure that includes a plurality of data items, and an entirety parameter that is dependent upon a plurality of security identifiers associated with the data items (FIG. 2; page 9, lines 3-17).

As claimed in dependent claim 18, the storage medium further includes a plurality of other entirety parameters, each of the plurality of other entirety parameters being dependent upon an associated plurality of security identifiers (page 11, line 20 through page 12, line 3).

As claimed in independent claim 25, the invention comprises an encoder (110 of FIG. 1) of content material that includes a selector (112), a binder (116), and a recorder (114). The selector selects a plurality of data items comprising the content material, each of the plurality of data items having an associated security identifier that is configured such that a modification of the data item effects a modification of the security identifier (page 11, lines 7-19). The binder creates an entirety parameter based on a plurality of the security identifiers (page 7, lines 18-23), and the recorder combines the entirety parameter with the plurality of data items to form a self-referential data set that is stored on a recorded medium (page 9, lines 3-17).

As claimed in dependent claim 32, the binder also creates a plurality of other entirety parameters, each of the plurality of other entirety parameters being based on an associated plurality of security identifiers, and the recorder combines the plurality of other entirety parameters with the data set (page 11, line 20 through page 12, line 3). As noted above, this allows for the determination of whether an entirety of the data set is likely to be present based on one or more of the plurality of entirety parameters (page 12, lines 22-24).

As claimed in independent claim 33, the invention comprises a decoder of content material (120 of FIG. 1; page 12, lines 4-30)) comprising a renderer (122), and an entirety checker (126). The renderer receives an entirety parameter corresponding to the content material, and a plurality of security identifiers corresponding to data items in the content material, upon which the entirety parameter is based (420-430 of FIG. 4; page 12, lines 9-17). The entirety checker determines an entirety value based on the plurality of security identifiers (440 of FIG. 4; page 12, lines 17-19), and precludes rendering of the content material from the source based on a correspondence between the entirety value and the entirety parameter (445 of FIG. 4; page 12, lines 19-21).

As claimed in dependent claim 34, the entirety parameter is randomly selected from a set of entirety parameters (410 of FIG. 4; page 12, lines 7-10), each entirety parameter of the set of entirety parameters having an associated set of security identifiers.

VI. ISSUES TO BE REVIEWED ON APPEAL

Claims 1-40 stand rejected under 35 U.S.C. 103(a) over Kurowski (USP 6,553,127) and Leighton (USP 5,949,885).

VII. ARGUMENT

Rejection under 35 U.S.C. 103(a) over Kurowski and Leighton

Claims 1-8

Claim 1, upon which claims 2-8 depend, comprises a method for discouraging theft of content material that includes collecting a plurality of data items comprising the content material to form a data set, each of the plurality of data items having an associated security identifier that is configured such that a modification of the data item effects a modification of the security identifier, creating an entirety parameter based on a plurality of the security identifiers; and including the entirety parameter in the data set to facilitate a preclusion of processing of a select data item of the plurality of data items in the absence of an entirety of the data set.

The Office action acknowledges that Kurowski does not disclose creating an entirety parameter based on a plurality of security identifiers (Final Office action, page 3, lines 11-13).

The Office action asserts that Leighton teaches creating an entirety parameter at column 5, line 66 through column 6, line 16. In the Advisory action, the Examiner asserts that Leighton's offset watermark vector W is interpreted as the entirety parameter. The applicants respectfully disagree with this characterization of Leighton.

Leighton teaches that some protection schemes use different watermarks on different copies of protected material to identify, for example, different purchasers of the material (Leighton, column 1, lines 34-43). Leighton notes, however, that an averaging of two different copies of the protected material having two different watermarks is likely to destroy the watermark, thereby obviating the protection (Leighton, column 1, lines 56-63).

Leighton teaches that an averaging attack will be ineffective if the different watermarks used in the different copies are uncorrelated. Leighton teaches the creation of a random offset watermark vector W that is added to a baseline watermark vector (Leighton, column 3, lines 44-55). Each different copy of the material receives a different random offset watermark vector W (Leighton, column 4, lines 42-65). Leighton specifically and repeatedly teaches that the security of Leighton's approach is based on the offset watermark vector W being random: "The scheme is immune to collusion because the watermark is random and because different watermarks are uncorrelated" (Leighton, column 4, lines 7-10). In a first embodiment, in order to determine whether a watermark is present in the material, the particular random offset vector W that was used to watermark the data is provided with the data (Leighton, column 5, lines 50-65). In a second embodiment, predefined data is mapped to the offset watermark vector W via a random hash function (Leighton, column 5, lines 66-67), so that all of the different random watermark vectors W can be recreated locally at a receiver for comparison with the derived watermark vectors (Leighton, column 6, lines 12-16). Leighton specifically teaches that the mapping to the offset watermark vector W should be a mapping into a sequence of independent Gaussian offsets to provide a random offset vector (Leighton, column 6, lines 23-34).

The applicants respectfully maintain that a randomly generated offset watermark vector as taught by Leighton does not correspond to an entirety parameter that is based on security parameters associated with data items in a data set, as specifically claimed by the applicants. In the embodiment cited in the final Office action, Leighton teaches a hash function that maps an identifier of the content material to a sequence of apparently random numbers based on information that is added to the content material, such as a copyright notice. Of particular note, neither the identifier of the content material nor the sequence of random numbers can be said to be security identifiers that are associated with data item comprising the content material.

Further, as discussed below, the applicants maintain that Leighton's randomly generated offset watermark does not constitute an entirety parameter as the term is used in the applicants' specification and as it is used in claim 1. Specifically, Leighton's randomly generated offset watermark will not facilitate a determination of whether an entirety of the data set is present. In particular, the absence or substitution of different data items in the received data set will result in a determination by Leighton that the material is not watermarked, and thereby freely available for rendering.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest creating an entirety parameter based on a plurality of the security identifiers; and including the entirety parameter in the data set to facilitate a preclusion of processing of a select data item of the plurality of data items in the absence of an entirety of the data set, as specifically claimed in claim 1, the applicants respectfully maintain that claims 1-8 are patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claim 8

Claim 8, which is dependent upon claim 1, recites creating a plurality of other entirety parameters, each of the plurality of other entirety parameters being based on an associated plurality of security identifiers, and including the plurality of other entirety parameters in the data set to further facilitate a preclusion of processing of each data item in the absence of an entirety of the data set.

The Office action acknowledges that Kurowski does not disclose creating an entirety parameter based on a plurality of security identifiers (Final Office action, page 3, lines 11-13).

The Office action cites Leighton, column 7, line 62 through column 8, line 10, for teaching the creation of multiple entirety parameters. The applicants respectfully disagree with this characterization of Leighton.

At the cited text, Leighton teaches the repeated encoding of a "Do not copy" watermark throughout the content material, using the aforementioned hash function to map this message to a random offset watermark vector.

The applicants respectfully maintain that neither the repeated "Do not copy" text nor the random offset watermark vectors can be said to correspond to a plurality of entirety parameters that are based on a plurality of security identifiers of data items in the data set.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest creating a plurality of other entirety parameters to further facilitate a preclusion of processing of each data item in the absence of an entirety of the data set, as specifically claimed in claim 8, the applicants respectfully maintain that claim 8 is patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claims 9-16

Claim 9, upon which claims 10-16 depend, claims a method of decoding content material from a source comprising: reading an entirety parameter and a plurality of security identifiers from the source, upon which the entirety parameter is based, each security identifier corresponding to a data item of the content material, determining an entirety value based on the plurality of security identifiers, and rendering the content material from the source in dependence upon a correspondence between the entirety value and the entirety parameter.

The Office action acknowledges that Kurowski does not disclose reading an entirety parameter based on a plurality of security identifiers (Final Office action, page 5, second to last paragraph).

The Office action asserts that Leighton teaches reading an entirety parameter from a source of the content material and determining an entirety value based on a plurality of security identifiers at column 5, line 65 through column 6, line 16. The applicants

disagree with this characterization of Leighton, based on the remarks above regarding Leighton, and based on the following remarks.

At the cited text of Leighton, Leighton teaches the use of a hash function to create a random offset watermark vector that is encoded with the data. Leighton specifically teaches that the purpose of this hash method is to avoid having to communicate the watermark with the data. Thus, even assuming in argument that Leighton's random offset watermark vector can be said to correspond to the applicants' claimed entirety parameter, Leighton specifically teaches against having to read this entirety parameter from the source of the content material.

The applicants again note that the random offset watermark vector of Leighton is not based on security identifiers that are associated with data items in a data set.

Further, the applicants note that Leighton does not teach a determination of an entirety value that is compared to an entirety parameter that is read from a source. Leighton teaches the determination of a correlation between the embedded watermark and the original offset watermark, but is silent with regard to determining an entirety value based on the plurality of security identifiers that are read from the source. The Office action is silent with regard to identifying an element in Leighton that corresponds to the claimed entirety value.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest reading an entirety parameter from a source of the content material and determining an entirety value based on a plurality of security identifiers, as specifically claimed in claim 9, the applicants respectfully maintain that claims 9-14 are patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claim 10

Claim 10, which is dependent upon claim 9, claims a random selection of the entirety parameter from a set of entirety parameters, each entirety parameter of the set of entirety parameters having an associated set of security identifiers.

The Office action cites Leighton's column 5, line 66 through column 6, line 5 for this teaching. The applicants respectfully note, however, that the cited text refers to the aforementioned random hash function that Leighton uses to create the random watermark vector, and does not refer to a random selection from a plurality of items. Specifically,

the cited text is silent with regard to randomly selecting the entirety parameter from a plurality of entirety parameters.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest a random selection of the entirety parameter from a set of entirety parameters, as specifically claimed in claim 10, the applicants respectfully maintain that claim 10 is patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claims 17-24

Claim 17, upon which claims 18-24 depend, claims a storage medium that is configured to contain content material, the storage medium comprising a data structure that includes: a plurality of data items, each data item having an associated security identifier, and an entirety parameter that is dependent upon a plurality of the security identifiers; wherein ... the entirety parameter facilitates a determination of whether an entirety of the plurality of data items is present on a subsequent copy of at least a portion of the plurality of data items.

The Office action acknowledges that Kurowski does not disclose an entirety parameter based on a plurality of security identifiers (Final Office action, page 6, last paragraph).

The Office action asserts that Leighton teaches an entirety parameter based on a plurality of security identifiers at column 5, lines 66 through column 6, line 6. The applicants disagree with this assertion, based on the remarks above regarding Leighton, and based on the following remarks.

The applicants respectfully maintain that Leighton's random offset watermark vector is not dependent upon security identifiers associated with data items in a data structure on a storage medium.

The applicants further maintain that the cited text of Leighton specifically teaches a method of forming a data structure that does not include the random offset watermark vector that the Office action asserts corresponds to the entirety parameter that is specifically claimed to be contained in the data structure.

The applicants further maintain that Leighton's random offset watermark vector does not facilitate a determination of whether an entirety of the data set is present on a

copy of the data items. The applicants respectfully maintain that if the sections containing Leighton's watermarks are removed from the data set, Leighton's device will find no correlation between any of the sets of random watermarks and the (smaller) data set, and will determine that the material is not watermarked, and is therefore freely renderable. In the context of songs of an album, if Leighton's watermark is distributed among the songs, and a single song that contains only a portion of Leighton's watermark is ripped from the album, it is unlikely that Leighton's device will detect a correlation between that portion and the offset watermark vector, because of the absence of all the other portions that contribute to the determination of a correlation (Leighton's column 4, line 66 through column 5, line 37).

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest a storage medium that includes an entirety parameter that is dependent upon a plurality of the security identifiers, as specifically claimed in claim 17, upon which claims 18-24 depend, the applicants respectfully maintain that claims 17-24 are patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claim 18

Claim 18, which is dependent upon claim 17, claims a storage medium that includes a plurality of other entirety parameters, each of the plurality of other entirety parameters being dependent upon an associated plurality of security identifiers.

As with regard to claim 8, the Office action cites Leighton, column 7, line 62 through column 8, line 10, for teaching the creation of multiple entirety parameters. At the cited text, Leighton teaches the repeated encoding of a "Do not copy" watermark throughout the content material, using the aforementioned hash function to map this message to a random offset watermark vector.

The applicants respectfully maintain that neither the repeated "Do not copy" text nor the random offset watermark vectors can be said to correspond to a plurality of entirety parameters that are based on a plurality of security identifiers of data items in the data set.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest a storage medium that includes a plurality of entirety parameters that are dependent upon associated pluralities of security identifiers, as specifically claimed in

claim 18, the applicants respectfully maintain that claim 18 is patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claims 25-32

Claim 25, upon which claims 26-32 depend, claims an encoder of content material comprising a selector that selects a plurality of data items comprising the content material, each of the plurality of data items having an associated security identifier, a binder that creates an entirety parameter based on a plurality of the security identifiers that facilitates a determination of whether an entirety of the plurality of data items is present, and a recorder that combines the entirety parameter with the plurality of data items to form a self-referential data set that is stored on a recorded medium.

The Office action relies on the basis of the rejection of claim 1 to support the rejection of claim 25 (Office action, page 7, second to last paragraph).

The applicants respectfully disagree with the asserted basis of rejection, based on the remarks above regarding Kurowski and Leighton, and based on the following remarks.

The Office action acknowledges that Kurowski does not disclose an entirety parameter based on a plurality of security identifiers, and relies upon Leighton for this teaching.

The Advisory action asserts that Leighton's offset watermark vector *W* at column 6, line 4, corresponds to the claimed entirety parameter.

Leighton's offset watermark vector *W* is a random vector that is generated by a random hash function based on "copyright and other information that the user desires to embed in the document (e.g. "This picture is the property of XYZ Corp., unauthorized copying is prohibited")" (Leighton, column 6, lines 1-3). This vector is not based on security identifiers associated with data items in the content material, and the purpose of this mapping is to avoid having to record the vector on the recorded medium: "Now, one need only remember the text, not the whole offset vector" (Leighton, column 6, lines 31-33). Because the offset watermark vector *W* can be regenerated locally based solely on the known text that was added to the content material, it cannot be said to be dependent upon security identifiers associated with data items within the content material.

That is, Leighton's offset watermark vector W is not dependent on security identifiers, as specifically claimed, and Leighton's offset watermark vector W is not recorded on the recording medium, as also specifically claimed.

Further, because the offset watermark vector W can be regenerated locally based solely on the known text that was added to the content material, it cannot be said to facilitate a determination of whether an entirety of the data set is present on a copy of the data items, as also claimed.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest a binder that creates an entirety parameter based on a plurality of the security identifiers that facilitates a determination of whether an entirety of the plurality of data items is present, nor a recorder that combines the entirety parameter with the plurality of data items to form a self-referential data set that is stored on a recorded medium, as specifically claimed in claim 25, upon which claims 26-32 depend, the applicants respectfully maintain that claims 26-32 are patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claim 32

Claim 32, which is dependent upon claim 25, claims that the binder further creates a plurality of other entirety parameters, each of the plurality of other entirety parameters being based on an associated plurality of security identifiers, and the recorder further combines the plurality of other entirety parameters with the data set to further facilitate a preclusion of processing of each data item in the absence of an entirety of the data set.

The Office action relies upon the basis of the rejection of claim 8 to support the rejection of claim 32 (Office action, third from last paragraph).

With regard to claim 8, the Office action cites Leighton, column 7, line 62 through column 8, line 10, for teaching the creation of multiple entirety parameters. At the cited text, Leighton teaches the repeated encoding of a "Do not copy" watermark throughout the content material, using the aforementioned hash function to map this message to a random offset watermark vector.

The applicants respectfully maintain that neither the repeated "Do not copy" text nor the random offset watermark vectors can be said to correspond to a plurality of

entirety parameters that are based on a plurality of security identifiers of data items in the data set.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest a plurality of entirety parameters, each of the plurality of entirety parameters being based on an associated plurality of security identifiers, as specifically claimed in claim 22, the applicants respectfully maintain that claim 22 is patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claims 33-40

Claim 33, upon which claims 34-40 depend, claims a decoder of content material that comprises a renderer that is configured to receive an entirety parameter corresponding to the content material, and a plurality of security identifiers upon which the entirety parameter is based, each security identifier corresponding to a data item of the content material, and an entirety checker that determines an entirety value based on the plurality of security identifiers, and precludes a rendering of the content material from the source in dependence upon a correspondence between the entirety value and the entirety parameter.

The Office action relies upon the basis of the rejection of claim 9 to support the rejection of claim 33 (Office action, page 7, last paragraph).

The applicants respectfully disagree with the asserted basis of rejection, based on the remarks above regarding Kurowski and Leighton, and based on the following remarks.

The Office action acknowledges that Kurowski does not disclose an entirety parameter based on a plurality of security identifiers, and relies upon Leighton for this teaching. The Advisory action asserts that Leighton's offset watermark vector W at page 6, line 4 corresponds to the claimed entirety parameter.

As noted above, Leighton teaches a method of creating a random offset watermark vector via a hash function specifically for the purpose of allowing the vector to be generated locally, based on a known text, so that communicating the vector to the decoder can be avoided.

Leighton specifically teaches that the offset vector can be locally regenerated based on a known text, therefore Leighton's offset vector cannot be said to be based on a plurality of security identifiers associated with data items in the content material, as specifically claimed.

Leighton also does not determine an entirety value based on a plurality of received security identifiers, and does not compare this determined entirety value with a received entirety parameter, as specifically claimed.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest receiving an entirety parameter that is based on a plurality of security identifiers, nor determining an entirety value that is compared to this entirety parameter, as specifically claimed in claim 33, upon which claims 34-40 depend, the applicants respectfully maintain that claims 34-40 are patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

Claim 34

Claim 34, which is dependent upon claim 33, claims that the renderer receives the entirety parameter based on a random selection from a set of entirety parameters, each entirety parameter of the set of entirety parameters having an associated set of security identifiers.

The Office action relies upon the basis of the rejection of claim 10 to support the rejection of claim 34 (Office action, page 8, first paragraph).

With regard to claim 10, the Office action cites Leighton's column 5, line 66 through column 6, line 5 for this teaching. As noted above, however, the cited text is silent with regard to randomly selecting the entirety parameter from a plurality of entirety parameters.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest a random selection of the entirety parameter from a set of entirety parameters, as specifically claimed in claim 34, the applicants respectfully maintain that claim 34 is patentable under 35 U.S.C. 103(a) over Kurowski and Leighton.

CONCLUSIONS

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest a method or device that encodes an entirety parameter that is based on a plurality of security identifiers associated with data items in content material, and because neither Kurowski nor Leighton, individually or collectively, teach or suggest a method or device that receives an entirety parameter that is based on a plurality of security identifiers associated with data items in content material, and because neither Kurowski nor Leighton, individually or collectively, teach or suggest a storage medium that includes an entirety parameter that is based on a plurality of security identifiers associated with data items in content material, the applicants respectfully request that the Examiner's rejection of claims 1-40 under 35 U.S.C. 103(a) over Kurowski and Leighton be reversed by the Board, and the claims be allowed to pass to issue.

Because neither Kurowski nor Leighton, individually or collectively, teach or suggest an encoding or decoding method or device or storage medium that includes a plurality of entirety parameters that are each based on a plurality of security identifiers associated with data items in content material, the applicants respectfully request that the Examiner's rejection of claims 8, 10, 18, 32, and 34 under 35 U.S.C. 103(a) over Kurowski and Leighton be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted,



Robert M. McDermott, Attorney

Registration Number 41,508

804-493-0707

APPENDIX
CLAIMS ON APPEAL

1. A method for discouraging a theft of content material comprising:

collecting a plurality of data items comprising the content material to form a data set that is sized to be sufficiently large so as to discourage a subsequent transmission of the data set via a limited bandwidth communications channel,

each of the plurality of data items having an associated security identifier that is configured such that a modification of the data item effects a modification of the security identifier,

creating an entirety parameter based on a plurality of the security identifiers; and
including the entirety parameter in the data set to facilitate a preclusion of processing of a select data item of the plurality of data items in the absence of an entirety of the data set.

2. The method of claim 1, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

3. The method of claim 1, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

4. The method of claim 3, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

5. The method of claim 3, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

6. The method of claim 1, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

7. The method of claim 1, wherein the entirety parameter is bound to a table of contents that is associated with the data set.

8. The method of claim 1, further including:

creating a plurality of other entirety parameters, each of the plurality of other entirety parameters being based on an associated plurality of security identifiers, and including the plurality of other entirety parameters in the data set to further facilitate a preclusion of processing of each data item in the absence of an entirety of the data set.

9. A method of decoding content material from a source comprising:

reading an entirety parameter corresponding to the content material from the source,

reading a plurality of security identifiers from the source, upon which the entirety parameter is based, each security identifier corresponding to a data item of the content material,

determining an entirety value based on the plurality of security identifiers,

rendering the content material from the source in dependence upon a correspondence between the entirety value and the entirety parameter.

10. The method of claim 9, wherein

reading the entirety parameter includes a random selection from a set of entirety parameters, each entirety parameter of the set of entirety parameters having an associated set of security identifiers.

11. The method of claim 9, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

12. The method of claim 9, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

13. The method of claim 12, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

14. The method of claim 12, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

15. The method of claim 9, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

16. The method of claim 9, wherein the entirety parameter is bound to a table of contents that is associated with the content material.

17. A storage medium that is configured to contain content material, the storage medium comprising

a data structure that includes:

a plurality of data items, each data item having an associated security identifier, and

an entirety parameter that is dependent upon a plurality of the security identifiers; and

wherein

each security identifier of the plurality of security identifiers is configured such that a modification of the data item effects a modification of the security identifier, and

the entirety parameter facilitates a determination of whether an entirety of the plurality of data items is present on a subsequent copy of at least a portion of the plurality of data items.

18. The storage medium of claim 17, further including

a plurality of other entirety parameters, each of the plurality of other entirety parameters being dependent upon an associated plurality of security identifiers.

19. The storage medium of claim 17, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

20. The storage medium of claim 17, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

21. The storage medium of claim 20, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

22. The storage medium of claim 20, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

23. The storage medium of claim 17, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

24. The storage medium of claim 17, wherein the entirety parameter is bound to a table of contents that is associated with the data set.

25. An encoder of content material comprising:

a selector that is configured to select a plurality of data items comprising the content material to form a data set that is sized to be sufficiently large so as to discourage a subsequent transmission of the data set via a limited bandwidth communications channel,

each of the plurality of data items having an associated security identifier that is configured such that a modification of the data item effects a modification of the security identifier,

a binder that is configured to create an entirety parameter based on a plurality of the security identifiers that facilitates a determination of whether an entirety of the plurality of data items is present, and

a recorder that is configured to combine the entirety parameter with the plurality of data items to form a self-referential data set that is stored on a recorded medium.

26. The encoder of claim 25, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

27. The encoder of claim 25, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

28. The encoder of claim 27, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

29. The encoder of claim 27, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

30. The encoder of claim 25, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

31. The encoder of claim 25, wherein

the binder is further configured to bind the entirety parameter to a table of contents that is associated with the data set.

32. The encoder of claim 25, wherein

the binder is further configured to create a plurality of other entirety parameters, each of the plurality of other entire parameters being based on an associated plurality of security identifiers, and

the recorder is further configured to combine the plurality of other entirety parameters with the data set to further facilitate a preclusion of processing of each data item in the absence of an entirety of the data set.

33. A decoder of content material comprising:

a renderer that is configured to receive:

an entirety parameter corresponding to the content material, and

a plurality of security identifiers upon which the entirety parameter is based, each security identifier corresponding to a data item of the content material,

an entirety checker, operably coupled to the renderer, that is configured to

determine an entirety value based on the plurality of security identifiers,

and

preclude a rendering of the content material from the source in

dependence upon a correspondence between the entirety value and the entirety parameter.

34. The decoder of claim 33, wherein

the renderer is further configured to receive the entirety parameter based on a random selection from a set of entirety parameters, each entirety parameter of the set of entirety parameters having an associated set of security identifiers.

35. The decoder of claim 33, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

36. The decoder of claim 33, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

37. The decoder of claim 36, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

38. The decoder of claim 36, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

39. The decoder of claim 33, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

40. The decoder of claim 33, wherein the entirety parameter is bound to a table of contents that is associated with the content material.